2016 年 4 月 4 日，星期一

研究聚焦：低价成为不法分子的温床

作者：Tazz。

执行摘要

2 月底，Talos 团队的一名研究员收到某域名经销商发送的一封促销电子邮件。于是，她在 3 月的第一周对这家经销商进行了评估。这封来自 Namecheap 的电子邮件声称可以提供大幅折扣的域名，价格只有 88 美分。我们收到这封电子邮件的时间颇有些让人感到巧合，因为我们目前正在开展特定的研究，以确定域名的定价和那些与恶意软件/网络钓鱼/垃圾邮件相关的域之间是否存在联系。本文将探讨大幅折扣域服务与违法活动之间的关系。就本文而言，恶意一词将包括恶意软件、网络钓鱼和垃圾邮件等恶意活动。

背景

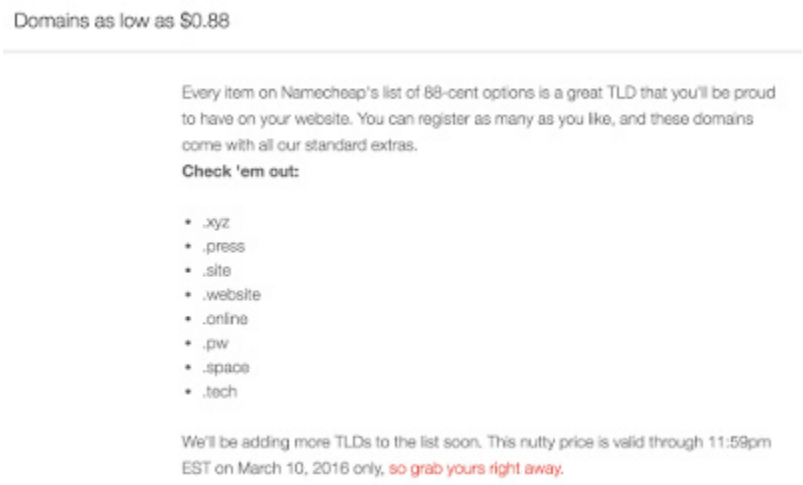
Talos 曾经就不法分子与廉价/免费服务之间相互吸引的关系展开调查。毫无疑问，在互联网上，我们花钱可以买到我们想要的东西。但是如果买的是廉价或免费的，很有可能会被不法分子利用。我们发现对于动态 DNS，这一理论很符合现实，并且我们看到当攻击者转向动态 DNS 时，许多不法分子都在利用廉价服务。有关更多内容，可参阅 https://blogs.cisco.com/security/dynamic-detection-of-malicious-ddns。

任何商人，无论好坏，都是以快速赚钱为目标。要达到这个目标，就必须追求投资回报最大化，并且/或者找到一个只需较低成本即可进入的市场。如果起步经费需要 5000 美元，那么大多数人就会望而止步，对犯罪分子而言更是如此。但是如果成本只需要 50 美元，甚至 5 美元，那么无疑就更有可能吸引很多人前来淘金。这套原则同样适用于在互联网上兴风作浪的不法分子。因此，考虑到这封电子邮件声称能够提供大幅折扣的顶级域名 (TLD)，Talos 团队设想了一个情况，我们来探讨一下。

假设：当域名价格小于或等于 1 美元时，注册量会增加，同时与 TLD 有关的恶意活动也会相应地增加。

交易

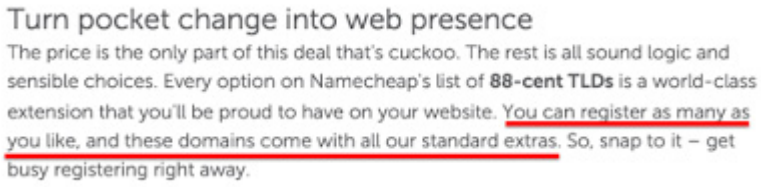
下面是 Namecheap.com 促销电子邮件的屏幕截图，宣传他们的低廉价格（88 美分）。



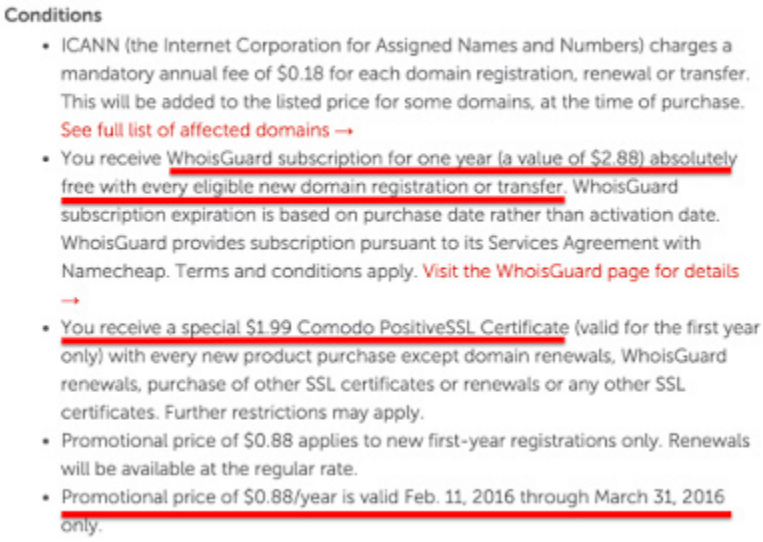
Namecheap 促销电子邮件的正文

我们在 3 月 21 日快速访问了他们的网站，发现这场本应该在 3 月 10 日截止“交易”非但没有像促销电子邮件里说的那样停止销售，反而为那些虎视眈眈的不法分子增加了 5 个充满诱惑力的条件。

第一，只需花费 88 美分就可以获得域名，与通常那些有数量限制的“好得让人无法抗拒”的交易不同，在这里，你想买多少就能买多少！



第二，优惠活动并没有如电子邮件中所述那样在 3 月 10 日结束。事实上，这次优惠持续了 50 天，直到 3 月 31 日才停止。



Conditions

- ICANN (the Internet Corporation for Assigned Names and Numbers) charges a mandatory annual fee of $0.18 for each domain registration, renewal or transfer. This will be added to the listed price for some domains, at the time of purchase. See full list of affected domains →
- You receive WhoisGuard subscription for one year (a value of $2.88) absolutely free with every eligible new domain registration or transfer. WhoisGuard subscription expiration is based on purchase date rather than activation date. WhoisGuard provides subscription pursuant to its Services Agreement with Namecheap. Terms and conditions apply. Visit the WhoisGuard page for details →
- You receive a special $1.99 Comodo PositiveSSL Certificate (valid for the first year only) with every new product purchase except domain renewals, WhoisGuard renewals, purchase of other SSL certificates or renewals or any other SSL certificates. Further restrictions may apply.
- Promotional price of $0.88 applies to new first-year registrations only. Renewals will be available at the regular rate.
- Promotional price of $0.88/year is valid Feb. 11, 2016 through March 31, 2016 only.

2016 年 3 月 21 日 Namecheap 的销售情况截图。

第三，WhoisGuard 会屏蔽注册者的详细信息，不仅免费向新域名购者提供，而且支持免费变更域名。为了让交易更加充满诱惑力，购买者甚至只需花费 1.99 美元即可获得合法的 SSL 证书。第五点也是最后一点，除了在电子邮件中列出的 8 种域名以外，还有其他 16 种域名可供选择。

来自 Namecheap.com 的 88 美分域名列表

Namecheap.com 的原始网页内容

值得注意的是，Namecheap 并不是以如此大幅的折扣提供域名的唯一商家。在我们的研究中，像前面介绍的 Namecheap 这样以低成本拉客的活动最早出现在 1 月 29 日，并一直持续到 2 月初。这表明其他很多提供商也在以不足 1 美元的价格提供 TLD（截图中反映的价格是 2016 年 1 月 29 日至 2 月 8 日期间的促销价格）。

top	alpnames.com	$0.40
win	alpnames.com	$0.45
accountant	alpnames.com	$0.60
bid	alpnames.com	$0.60
cricket	alpnames.com	$0.60
date	alpnames.com	$0.60
download	alpnames.com	$0.60
faith	alpnames.com	$0.60
loan	alpnames.com	$0.60
party	alpnames.com	$0.60
racing	alpnames.com	$0.60
review	alpnames.com	$0.60
science	alpnames.com	$0.60
trade	alpnames.com	$0.60
webcam	alpnames.com	$0.60
top	epik	$0.75
top	hexonet	$0.99
club	godaddy	$0.99
com	1and1	$0.99
info	1and1	$0.99
info	godaddy	$0.99
mobi	godaddy	$0.99
ninja	godaddy	$0.99
online	godaddy	$0.99
site	godaddy	$0.99
space	1and1	$0.99
space	godaddy	$0.99
tech	godaddy	$0.99
website	godaddy	$0.99
xyz	godaddy	$0.99
kred	Enom	$1.00
top	dynadot	$1.00
xyz	namecheap	$1.00

2016 年 1 月 29 日的各种折扣

躲在 WHOISGUARD 之后的是哪些人？

利用 Domain Tool Iris 产品，我们将 Namecheap 促销开始后前 40 天的销售情况与大幅折扣开始之前 40 天的销售情况进行了比较，得出了一些有趣的结论。数据反映的是所有经销商的情况，而不仅仅是 Namecheap。因为尽管 Namecheap 的广告促成了本文，但他们并不是唯一对 TLD 提供大幅折扣的零售商。需要注意的是，评估以下风险评分时，这些评分表示的是查询当天（3 月 21 日）计算所得的分数。因此，从 1 月 1 日开始为期 40-80 天的活动会影响 3 月 21 日所反映的风险评分。在评估 2 月 11 日到 3 月 21 日之间注册的域名的风险评分

时，我们仅考虑期限在 0 到 40 天的活动。如果把最开始的假设考虑其中，那么在此数据集里，我们预计风险评分大于等于 90 分的域名比例相当小（约二分之一）。然而，这种假设看起来只有在域名不使用 WhoisGuard 时才成立。

1 JAN - 10 FEB		
WHOISGUARD	TOTAL	W/ RS>=90
YES	72,643	1.78%
NO	1,106,126	4.46%
11 FEB - 21 MARCH		
WHOISGUARD	TOTAL	W/ RS>=90
YES	124,792	1.26%
NO	2,296,541	2.43%

来自 Domain Tool Iris 的数据

注册了 WhoisGuard 隐私的域数量增长了大约 58%，而风险评分 (RS) 大于或等于 90 的域的百分比保持相对不变，两组之间的差为 0.52%。没有注册 WhoisGuard 隐私的域数量增长了大约 48%，但是风险评分大于或等于 90 的域数量下降了几乎一半。

屏蔽网络流量

再来看看 Web 屏蔽的数据，我们发现在 2 月 11 日到 3 月 21 日期间，屏蔽流向其中一个打折出售的 TLD 的 URL 流量比 1 月 1 日到 2 月 10 日期间增长了 23%。我们还发现，在 1 月 1 日到 2 月 10 日期间，排名前 4 的 ANS 占据屏蔽含有一个大幅折扣 TLD 的 URL 总数的 85%；从 2 月 11 日到 3 月 21 日，被屏蔽的 ASN 数量几乎是以往的三倍，排名前 3 的网站依旧占据被屏蔽网站总数的大约 85%，保持不变。这并不奇怪，前三位的 ASN 与 OVH SAS、Google 和 CloudFlare 相一致。在评估与折扣域名相关的 Web 屏蔽时，两个窗口中排名前两位的 TLD 依旧相同，.xyz 压倒竞争对手占据领先优势，.pw 则屈居第三。TLD 的 .top 将 .site 击败出前三，在第二轮获得第二名。您是否注意到，从 .top 年初的活动以来，.top 域名在 Web 阻止中的数量是以往的三倍。在其他的相关研究中，我们看到钓鱼用户重度依赖 .top 域名，有关详细信息，请查看我们的这篇博文：http://blog.talosintel.com/2016/03/angler-slips-hook.html。

WEB BLOCKS			
1 JAN - 10 FEB		11 FEB - 21 MAR	
xyz	54.02%	xyz	51.69%
pw	21.44%	pw	24.34%
site	10.31%	top	18.87%
top	6.78%	bid	1.64%
space	2.54%	online	1.09%
download	2.21%	space	0.82%
club	1.54%	club	0.55%
online	0.33%	download	0.36%
website	0.33%	website	0.27%
win	0.33%	party	0.09%
accountant	0.11%	review	0.09%
party	0.06%	site	0.09%
bid	0.00%	tech	0.09%

有趣的是，在我们的数据集中，Namecheap 的一些大幅折扣域名在每个 TLD 的屏蔽率不到 0.9%，但他们却经常出现在垃圾邮件/病毒类型的电子邮件中。

电子邮件

首先让我们来看看大体情况，捕捉独特的垃圾邮件和病毒消息量。至于垃圾电子邮件，第二个窗口和第一个窗口相比，我们看到了略微的下降 (-14.71%)，但病毒电子邮件的增长令人惊讶 (+357.90%)。虽然让人感到困扰，但如果考虑到在我们所受到的威胁中，勒索软件也在不断增长，就可以理解了。在这两个日期范围中，两种恶意软件类别的净活动量合计增加了 3.76%。

我们再来详细了解一下仅与 TLD 子集相关的活动。TLD 子集的垃圾邮件和病毒电子邮件组合占 1 月 1 日到 2 月 10 日期间整个垃圾邮件和病毒电子邮件的 9.47%，在 Namecheap 的前 40 天销售期间（2 月 11 日到 3 月 21 日），仅占垃圾邮件和病毒电子邮件的总数 3.75%。我们随后决定进行更加深入的研究，以了解各个大幅折扣的 TLD 的“表现情况”。我们首先将每次屏蔽中出现的 TLD 的所有电子邮件包括在内，然后计算电子邮件中垃圾邮件/病毒电子邮件的百分比。下表列出每个 TLD 占在特定时间段里同一 TLD 的所有电子邮件的百分比。我们注意到 .top TLD 在垃圾邮件/病毒电子邮件的出现次数几乎翻番，但其他排名靠前的 TLD（例如 .date、.download、.xyz）实际上在逐渐减少。

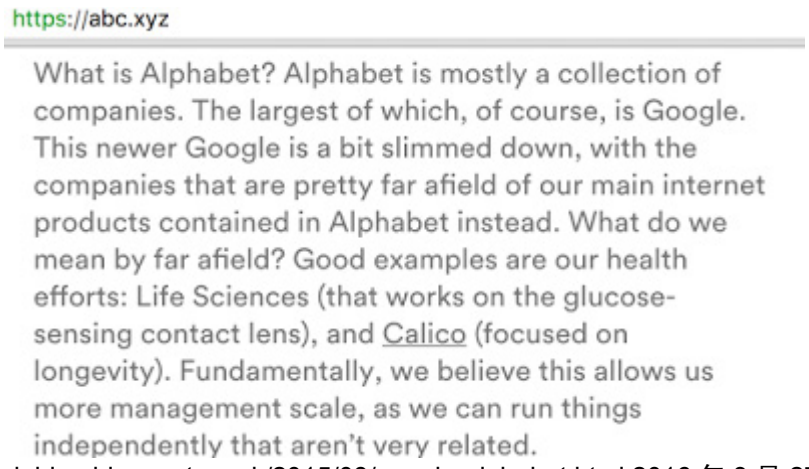
1 JAN - 10 FEB		11 FEB - 21 MAR	
.date	29.34%	*.top*	43.46%
.top	24.07%	*.download*	12.43%
.download	16.43%	*.date*	9.23%
.xyz	8.06%	*.website*	6.87%
.club	5.66%	*.review*	5.04%
.win	3.09%	*.racing*	3.35%
.review	2.75%	*.online*	3.28%
.racing	2.35%	*.win*	2.38%
.space	2.19%	*.xyz*	2.37%
.bid	1.93%	*.space*	2.19%
.faith	1.55%	*.bid*	1.72%
.online	0.60%	*.site*	1.51%
.webcam	0.33%	*.tech*	1.35%
.tech	0.30%	*.club*	1.14%
.party	0.28%	*.trade*	0.69%
.trade	0.26%	*.faith*	0.68%
.pw	0.25%	*.accountant*	0.59%
.accountant	0.24%	*.pw*	0.45%
.loan	0.09%	*.press*	0.44%
.science	0.09%	*.science*	0.44%
.site	0.07%	*.party*	0.15%
.website	0.05%	*.loan*	0.09%
.cricket	0.03%	*.webcam*	0.09%
.press	0.005%	*.cricket*	0.06%

百分比表示具有该 TLD 的电子邮件与具有打折 TLD 的电子邮件总数之间的比例。

恶意活动示例

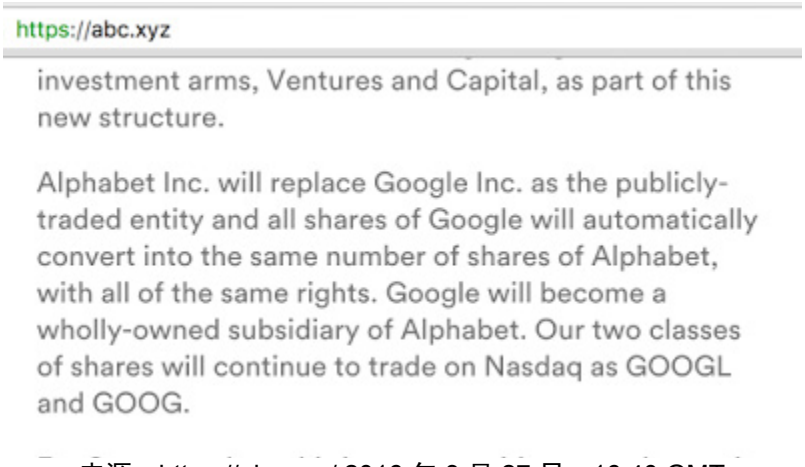
从以上数据可以看出，Alpnames 在年初抢在 Namecheap 前以大折扣力度先发制人，对域名 .top 和 .win 分别以 40 和 45 美分的价格进行销售。再来看看沙盒里符合自动判定为违规要求的样本，我们发现自 Namecheap 开始销售的前 40 天和销售开始前的 40 天，这些域都关联有更多恶意软件。但是，根据我们的研究，并没有哪一家经销商为 .pw 提供大幅折扣，但与其关联的恶意软件数量却始终是最高的。虽然我们还没有对 .pw TLD 相关恶意软件的受害者进行调查，但显而易见的是，众多用户会将其与密码重置域相关联，而在此域中就存在有窃取凭据的恶意软件。那么，为何与 .xyz 相关联的恶意活动量如此巨大？要知道，单凭扩

展名 .xyz 看起来的样子，很多人肯定会说：“你在开玩笑吗？这肯定不是真正的网站，对吧？”遗憾的是，这不但是真实的网站，甚至还有一些主要功能比 Google 还强大。对于 .xyz 域恶意活动的增加，有一个理论就是不法分子依靠 Google 查询的帮助来对 Google 的用户钓鱼。毕竟，公告显示，Google 将成为新母公司的全资子公司，xyz TLD 已经没有什么可以利用的价值。



来源：https://googleblog.blogspot.co.uk/2015/08/google-alphabet.html 2016 年 3 月 27 日，16:40 GMT

“Alphabet Inc. 将取代 Google Inc. 作为公开交易的实体，Google 的全部股份将自动转换为相同数量的 Alphabet 股份，全部拥有相同权益。Google 将成为 Alphabet 全资子公司”



来源：https://abc.xyz/ 2016 年 3 月 27 日，16:40 GMT

在观察与这些 TLD 关联的恶意软件时，有一件值得注意的事情就是并非所有在特定时间段出现在沙盒里的 TLD 都有与其关联的恶意软件。这并不意味着他们从未或将来也不会关联上恶意软件，这仅表明在开展此项研究的特定日期段期间没有恶意软件。视线回到 Namecheap 销售前的 40 天，我们可以看到 24 个域名中，实际上只有其中 13 个域名具有与恶意软件相关的统计学意义上的测量，平均每个域名每天有 164 个恶意软件样本。销售的前 40 天显示，15 个域名每天平均有 102 个恶意软件样本。总之，在 Alpnames 和 Namecheap（在此未标明其他经销商）为期 80 天的销售阶段里，我们看到被自动判定为恶意软件的样本有 10605 个。

请注意，此图表仅反映符合自动判断条件的样本，它并不意味着其他不符合默认自动判定标准的样本后期不会被发现具有恶意并判断出来。

TLD	1 JAN - 10 FEB	11 FEB - 21 MAR
accountant	0.00%	0.00%
bid	4.94%	7.33%
club	54.31%	37.07%
cricket	2.78%	0.00%
date	11.76%	0.00%
download	0.00%	0.00%
faith	0.00%	0.00%
loan	0.00%	0.00%
online	6.41%	26.04%
party	0.00%	7.69%
press	25.00%	42.86%
pw	4.35%	5.27%
racing	0.00%	0.00%
review	0.00%	0.00%
science	0.00%	3.23%
site	15.31%	11.18%
space	2.47%	7.01%
tech	0.00%	3.40%
top	6.35%	4.75%
trade	0.00%	50.00%
webcam	0.00%	0.00%
website	18.01%	2.80%
win	27.62%	18.67%
xyz	43.74%	15.75%
TOTAL	**6.80%**	**7.12%**
Total w/o .pw	**18.53%**	**11.70%**

独特的恶意软件样本与打折的 TLD 有关联活动，并被 Talos 沙盒自动判断出来

总结

不要前往无需前往的地点

不同组织的实施方式各不相同，但总的来说，还是建议在贵组织的风险承受能力范围内，阻止流向这些站点的流量。如果没有使用案例表明对某个站点有合法的或较大的需求，有些组织会选择在企业层面阻止整个 TLD。例如：位于 .xxx TLD 上的某网站并不是一家儿童友好型公司的员工需要访问的网站。不管怎样，如果您选择了这种方法，我们强烈建议您采用一套允许例外请求的高效流程。另一种方法是白名单，但它也有优缺点。基本的建议是与您的企业安全团队和主要利益相关方进行全面探讨，以确定哪种方法更适合贵组织。切记，忽略风险等同于接受风险。

您的好名声值得您拥有

许多组织在配置不同设备和过滤流量时都会考虑提供商/托管公司的声誉。在集团网络上阻止整个 ASN 的事情也不是没有听说过。由于域名价格低廉，并且您也不想因为自己的网站与不法分子的网站位于相同的域而冒着您的合法业务流量被阻止的风险，所以您并不想购买域。在不法之徒蜂拥至经销商/托管公司时，您可以把其比作每日都进食的小剂量砒霜。所需的时间并不多，但最终会让您的业务走向灭亡。

择邻而居

选择注册公司/托管公司的好处就是您可以在某种成度上选择您的邻居。就像找房子一样，如果您知道您的邻居恶贯满盈，就不会明知故犯还买此处的房子，除非您想铤而走险或者也是一个不法之徒。同样，您也希望和您所购买相同域的其他购买人都像您一样正直、诚实。如果您购买的是太过廉价的产品，那么这种机会就真的消失殆尽了。例如，我们看看 2 月份的特定 TLD (.download)，恶意域名分属 42 家不同供应商，其中 73% 属于 Alpnames 的资产。巧合的是，Alpnames 的价格（60 美分）也是最低的。然而另一家以 23.99 欧元（大约 26.15 美元）提供 .download 的提供商 Black Knight 就完全没有报告有不良域名。事实上，我们发现，在 Black Knight 提供的 327 个 TLD 中，最便宜的 TLD 是 .info，价格为 1.99 欧元（大约 2.17 美元）。但在域名工具中，没有注册域所反映的风险评分大于等于 90 分。这就是我想要的邻居。面对现实吧，如果不法之徒伴随您左右，与您共享同一客户空间，甚至他们还决定利用自己的资产作为入侵您的支点，好吧，您只能希望自己已经做好了应对准备。所以，如果不喜欢您的四邻，那您可能是选错了邻居。

在把这一切都考虑进来以后，最重要的主题就是大幅折扣（廉价）的互联网服务和犯罪/恶意活动之间有着无可争辩的关联。该活动范围和严重性可能包括从不想收到的垃圾邮件到彻底牺牲重要数据的各种危害。尽管如此，如果在互联网上有价格低廉或免费的东西，那么毫无疑问，它就会被用于从事不法活动。此外，上市销售域名时，尤其对价格不足 1 美元的域名来说，域名注册量和“不法分子”的数量也会大量增加。我们鼓励客户和所有用户采取预防措施来保护其资产。对于商业用户来说尤为如此，应进行充分的风险评估，并确定合法业务

是否需要访问这些“非标准”TLD，如果不需要，在分层安全模型实施配置，过滤电子邮件和网络流量，并实施主机级别的保护，最重要的是，备份您的资产！！

发布者：TAZZ；发布时间：下午 12:04
标签：廉价域、DDNS、折扣域、动态 DNS、GTLD、恶意活动、恶意攻击者、恶意软件、研究聚焦、SPAM、TLD